CLAIMS

What is claimed is:

1. In a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a method of establishing a connection to the private network resource while balancing authentication processing requirements between a client and the firewall to mutually guard against denial of service attacks, the method comprising the acts of:

receiving, by the firewall, a request from the client to access the private network resource, wherein the request from the client is made to the private network resource without any knowledge of the firewall;

requesting, by the firewall, the client to provide one or more client credentials to authenticate the client;

sending, by the firewall, one or more firewall credentials to authenticate the firewall, wherein generating the one or more firewall credentials consumes some level of limited firewall processing resources;

receiving one or more client credentials at the firewall, wherein generating the one or more client credentials consumes some level of limited client processing resources similar in magnitude with the consumption of the limited firewall processing resources;

verifying, by the firewall, the one or more client credentials;

establishing a secure channel for accessing the private network resource in response to the verification of the one or more client credentials; and

forwarding data from the client destined to the private network resource through the firewall using the secure channel.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

2. The method of claim 1, wherein the step of verifying comprising the act of:

continuing an exchange of credentials between the client and the firewall to incrementally increase a level of trust between the client and the firewall until a predefined threshold of trust is reached.

3. The method of claim 1, wherein the private network resource is one of a host, gateway or server.

4. The method of claim 1, wherein the only data passed through the firewall from the client are those packets of data destined to the private network resource.

5. The method of claim 1, further comprising the act of:

establishing a connection with a resource of a separate private network while simultaneously maintaining the secure channel of the private network.

6. The method of claim 1, further comprising the act of:

establishing a connection with another private network resource while simultaneously maintaining the secure channel of the private network.

7. The method of claim 1, wherein the act of forwarding the data from the client to the private network resource is accomplished through the use of an authenticated channel, the method further comprising the act of:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

signing, by the firewall, the packets of data from the client destined to the private network resource, wherein the singing indicates that the client has passed one or more security check implemented in the firewall.

8. The method of claim 7, further comprising the act of:

discarding unsigned packets of data received by the protected private network resource.

9. The method of claim 1, wherein the one or more client credential received is selected from at least one of a user's name, client's IP address, password, passport, smart-card or credit card number.

10. The method of claim 1, wherein the request, by the firewall, for the client to provide one or more client credentials is a question, and wherein the one or more client credentials received is an answer to the question.

11. The method of claim 1, wherein the client is a second firewall.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

12. In a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a method of establishing a connection to the private network resource while balancing authentication processing requirements between a client and the firewall to mutually guard against denial of service attacks, the method comprising steps for:

initiating a series of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein each authentication transaction incrementally increases a level of trust between the client and the firewall until the authentication of the client and the firewall are sufficiently verified;

for each of the series of authentication transactions:

authenticating to the client in accordance with one of the series of authentication transactions; and

challenging the client to authenticate in a manner requiring similar processing burdens; and

granting the client access to the private network resource through the firewall upon completing the series of authentication transactions..

13. The method of claim 12, wherein the step for challenging the client to authenticate comprises the acts of:

requesting, by the firewall, the client to provide one or more client credentials;

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

receiving one or more client credentials at the firewall; and

verifying, by the firewall, the one or more client credentials.

14. The method of claim 13, wherein the one or more credentials authenticated is at least one of a user's name, client's IP address, password, passport, smart-card or credit card number.

15. The method of claim 13, wherein the request, by the firewall, for the client to provide one or more client credentials is a question, and wherein the one or more client credentials received is an answer to the question.

16. The method of claim 12, wherein once the client is granted access to the private network resource the only data passed through the firewall from the client are those packets of data destined to the private network resource.

17. The method of claim 12, wherein the step for granting includes the act of:

establishing an authenticated channel between the firewall and the private network resource, wherein the authenticated channel is established through signing the data from the firewall.

18. The method of claim 17, further comprising the act of:

discarding any unsigned packets of data received by the private network resource.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

19. The method of claim 12, wherein the private network resource is one of a host, gateway or server.

20. The method of claim 12, wherein the client is a second firewall.

21. The method of claim 12, further comprising the act of:

establishing a connection with another resource of a separate private network while simultaneously maintaining a secured channel between the firewall and the client.

22. The method of claim 12, further comprising the act of:

establishing a connection with another private network resource while simultaneously maintaining a secured channel between the firewall and the client.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

23. In a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a computer readable media carrying computer executable instructions that implement a method of establishing a connection to the private network resource while balancing authentication processing requirements between a client and the firewall to mutually guard against denial of service attacks, the method comprising the acts of:

receiving, by the firewall, a request from the client to access the private network resource, wherein the request from the client is made to the private network resource without any knowledge of the firewall;

requesting, by the firewall, the client to provide one or more client credentials to authenticate the client;

sending, by the firewall, one or more firewall credentials to authenticate the firewall, wherein generating the one or more firewall credentials consumes some level of limited firewall processing resources;

receiving one or more client credentials at the firewall, wherein generating the one or more client credentials consumes some level of limited client processing resources similar in magnitude with the consumption of the limited firewall processing resources;

verifying, by the firewall, the one or more client credentials;

establishing a secure channel for accessing the private network resource in response to the verification of the one or more client credentials; and

forwarding data from the client destined to the private network resource through the firewall using the secure channel.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

24. The method of claim 23, wherein the step of verifying comprising the act of:

continuing an exchange of credentials between the client and the firewall to incrementally increase a level of trust between the client and the firewall until a predefined threshold of trust is reached.

25. The method of claim 23, wherein the private network resource is one of a host, gateway or server.

26. The method of claim 23, wherein the only data passed through the firewall from the client are those packets of data destined to the private network resource.

27. The method of claim 23, further comprising the act of:

establishing a connection with a resource of a separate private network while simultaneously maintaining the secure channel of the private network.

28. The method of claim 23, further comprising the act of:

establishing a connection with another private network resource while simultaneously maintaining the secure channel of the private network.

29. The method of claim 23, wherein the act of forwarding the data from the client to the private network resource is accomplished through the use of an authenticated channel, the method further comprising the act of:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

signing, by the firewall, the packets of data from the client destined to the private network resource, wherein the singing indicates that the client has passed one or more security check implemented in the firewall.

30. The method of claim 29, further comprising the act of:

discarding unsigned packets of data received by the protected private network resource.

31. The method of claim 23, wherein the one or more client credential received is selected from at least one of a user's name, client's IP address, password, passport, smart-card or credit card number.

32. The method of claim 23, wherein the request, by the firewall, for the client to provide one or more client credentials is a question, and wherein the one or more client credentials received is an answer to the question.

33. The method of claim 23, wherein the client is a second firewall.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

34. In a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a computer readable media carrying computer executable instructions that implement a method of establishing a connection to the private network resource while balancing authentication processing requirements between a client and the firewall to mutually guard against denial of service attacks, the method comprising steps for:

initiating a series of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein each authentication transaction incrementally increases a level of trust between the client and the firewall until the authentication of the client and the firewall are sufficiently verified;

for each of the series of authentication transactions:

authenticating to the client in accordance with one of the series of authentication transactions; and

challenging the client to authenticate in a manner requiring similar processing burdens; and

granting the client access to the private network resource through the firewall upon completing the series of authentication transactions.

35. The method of claim 34, wherein the step for challenging the client to authenticate comprises the acts of:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

requesting, by the firewall, the client to provide one or more client credentials;

receiving one or more client credentials at the firewall; and

verifying, by the firewall, the one or more client credentials.

36. The method of claim 35, wherein the one or more credentials authenticated is at least one of a user's name, client's IP address, password, passport, smart-card or credit card number.

37. The method of claim 35, wherein the request, by the firewall, for the client to provide one or more client credentials is a question, and wherein the one or more client credentials received is an answer to the question.

38. The method of claim 35, wherein once the client is granted access to the private network resource the only data passed through the firewall from the client are those packets of data destined to the private network resource.

39. The method of claim 34, wherein the step for granting includes the act of:

establishing an authenticated channel between the firewall and the private network resource, wherein the authenticated channel is established through signing the data from the firewall.

40. The method of claim 39, further comprising the act of:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

discarding any unsigned packets of data received by the private network resource.

41. The method of claim 34, wherein the private network resource is one of a host, gateway or server.

42. The method of claim 34, wherein the client is a second firewall.

43. The method of claim 34, further comprising the act of:

establishing a connection with another resource of a separate private network while simultaneously maintaining a secured channel between the firewall and the client.

44. The method of claim 34, further comprising the act of:

establishing a connection with another private network resource while simultaneously maintaining a secured channel between the firewall and the client.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

45. In a private network comprising a server and a firewall, which acts as a gateway by controlling access to the server, a method of providing access to the server through the firewall without a client knowing about the firewall, the method comprising the acts of:

receiving at the firewall, an access request from the client that is directed to the server because the client does not know that the firewall operates as a gateway for the server;

generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall;

the firewall sending a request for the client to authenticate to the firewall, the request including the one or more firewall authentication credentials so that the client knows of the level of trust between the server and the firewall without having to make a separate request;

receiving at the firewall, one or more authentication credentials from the client;

the firewall verifying the one or more client authentication credentials; and

thereafter, allowing the client to access the server through the firewall.

46. A method as recited in claim 45, further comprising the acts of:

establishing a secure connection between the firewall and the server; and

forwarding data received from the client to the server over the secure connection.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

47. A method as recited in claim 45, further comprising an acts of:

receiving at the firewall data from the client;

the firewall signing the received data; and

the firewall forwarding the signed data to the server.

48. A method as recited in claim 45, wherein the server comprises a host or a gateway.

49. A method as recited in claim 45, wherein the client comprises another firewall.

50. A method as recited in claim 45, wherein the client maintains a separate connection with another server, and wherein only data intended for the private network passes through the firewall.

51. A method as recited in claim 50, wherein the other server is part of a separate and distinct virtual private network.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111